UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,859	02/27/2002	Melissa W. Dunn	MS# 180490.1 (MSFT 4969)	8746

321 7590 02/24/2006		EXAMINER	
SENNIGER POWERS		JOO, JOSHUA	
ONE METROPOLITAN SQUARE			
16TH FLOOR	ART UNIT		PAPER NUMBER
ST LOUIS, MO 63102	2154		

DATE MAILED: 02/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/084,859	DUNN, MELISSA W.
	Examiner	Art Unit	
	Joshua Joo	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 December 2005</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-19,21-23,25-30 and 32-46* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5-19, 21-23, 25-30, and 32-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

Response to RCE/Amendment filed on 12/5/2005

1.   Claims 1-3, 5-19, 21-23, 25-30, and 32-46 are presented for examination.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3.   Claims 5, 32, and 33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

   i)   As per claim 5, claim 5 depends on the previously canceled claim 4, wherein the limitation of claim 5 is cited in claim 1.

   ii)   As per claims 32 and 33, both claims depend on the previously canceled claim 31. Both claims will depend on claim 29 for this office action.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1-3, 5, 7, 9, 14-15, 19, 21, 29-30, 32-35, 38-41, 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Desai, US Patent #6,820,204, in view of Cheung, US Publication #2005/0240622 (Cheung hereinafter).

6.   As per claims 1, 5, 14, 15, 19, 21, 29-30, 32-33, 38-41, and 44, Desai teaches

substantially the invention as claimed including a method, media having computer instructions

(Col 10, line 62 - Col 11, line 51. Software and hardware.), apparatus, and system for

controlling access to user-specific information for use in connection with a network computing

environment including a web-services provider providing a web-based software service. Desai's

teachings comprising:

        providing a user access to a service provided by the web-services provider, said web-

services provider maintaining a data store of user-specific information associated with the user

in connection with the service (Col 8, lines 27-41. Web application. Information exchange

system (IES) stores profile data of users.), said web-services provider maintaining an access

control list identifying when the user grants a form of access to a client wherein the form of

access granted to the client is limited to certain user-specific information (Col 9, lines 10-17.

User selectively grants data by element-by-element basis.);

        providing a client access to the service provided by the web-services provider, said client

seeking access to some of the user-specific information maintained in the data store (Col 9,

lines 18-22. Vendor accesses user profile.);

        obtaining an access request message from the client and directed to the software

service requesting user-specific information, said request message including an access request

parameter indicating the client's requested form of access to the user-specific information in the

data store (Col 13, lines 39-52; Col 14, lines 63-67. Requests access user profile, request

includes user ID.);

        comparing the access request parameter to an access control list associated with the

software service, said access control list identifying whether the user has granted the form of

access requested by the client (Col 13, lines 39-43; Col 14, lines 1-12. Checks user ID with

allowed level of access.);

permitting the client to have access to the requested user-specific information in the data

store if the user has granted the form of access requested by the client (Col 14, lines 18-20; Col

15, lines 8-12. Grants access to profile element-by-element basis.); and

determining an intended use by the client of the requested user-specific information in

the data store (Col 9, lines 22-29. Business contact, telemarketing. Col 13, lines 9-21.

Merchant requesting credit card.);

comparing the determined intended use by the client with a default access control

instruction (Col 9, lines 27-31. Telemarketer is denied access.);

updating the access control list to permit the client to have access to the requested user-

specific information in the data store (Col 13, lines 25-38; Col 14, lines 63-67. third party user

ID is associated with selected data elements.);

transmitting a fault response to the client if the default access control instruction does

not permit the determined intended use (Col 9, line 27-31; Col 15, lines 1-7. Denied access.);

and

wherein the user communicates with the web-services provider via a network

communication device having a display interface and a selection interface (Col 8, lines 56-67.

User selectively grants access to third parties. Col 10, lines 20-32. User communicates with

IES.), the method further comprising:

7.   Desai does not teach:

invoking an access control engine if the user has not previously granted the form of

access requested by the client, said access control engine:

updating the access control list to permit the client to have access to the requested user-

specific information in the data store if the default access control instruction permits the

determined intended use; and

generating an option list in response to the client's request for user-specific information

having at least one entry therein based on the determined intended use by the client of the

requested user-specific information in the data store;

displaying to the user on the display interface of the network communication device an

option menu reflecting the generated option list, said option menu prompting the user to accept

or reject at least one option using the selection interface of the network communication device,

and said option list generated in response to the client's request for user-specific information;

receiving from the network communication device a selection signal indicative of whether

the user accepted or rejected the at least one option; and

creating an access control rule based on the received selection signal, said access

control defining the extent of access to the requested user-specific information in the data store

granted to the client.

8.   Cheung teaches of invoking an access control engine in response to the client's request

if the client has not been granted the form of access; updating the access control list to permit

the client to have access to the requested information; requesting the administrator that the

access level be changed to allow for greater access; and updating the access level according to

the client's request (Paragraph 0038).

9.   Even though Cheung does not teach that the client provides the intended use, thereby

creating an option list containing the intended use of the information, Cheung does teach of

requesting by clients for a greater level of access if access is not granted, and Desai teaches of

providing the intended use for gaining access to the user-specific information. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai and Cheung and to provide the intended use in addition to the request for a greater level of access because doing so would improve the teachings of Desai by providing dynamic changing of clients' access levels and providing more control of information by the user.

10.   As per claim 2, Desai teaches the method of claim wherein comparing the determined intended use by the client with the default access control instruction further comprises comparing the client's requested form of access to the default access control instruction to determine if the default access control instruction permits the requested form of access (Col 9, lines 26-31; Col 15, lines 1-3. Third party not granted access is not allowed access to user profile.).

11.   As per claim 3, Desai teaches the method of claim 1 wherein the client's requested form of access to the user-specific information in the data store identifies a desired subject matter to be accessed and a method of accessing the desired subject matter and wherein comparing the determined intended use by the client with the default access control instruction further comprises: determining if the default access control instruction permits the client to access the desired subject matter; and determining if the default access control instruction permits the identified method of accessing the desired subject matter (Col 9, lines 22-25; Col 13, lines 39-42. Grants or denies third parties by element-by-element basis.).

12.   As per claims 7 and 35, Desai teaches the invention further comprising authenticating a

digital identity of the user and denying access to the requested user-specific information in the

data store if the digital identity of the user is not authenticated (Col 13, lines 25-42. Key. Col

14, lines 1-11, 65-67. Password and user ID.).

13.   As per claim 9, Desai teaches the method of claim 1 further comprising:

        determining if the client has an access subscription right to the requested user-specific

information in the data store (Col 9, lines 42-52. Send profile data to allowed vendors.); and

permitting the client to have access to the requested user-specific information in the data store if

the client has access subscription right to the requested user-specific information in the data

store (Col 9, lines 40-42. Registered user provides access to vendors.).

14.   As per claim 34, Desai does not teach the system of claim 33 wherein the access control

engine denies the requested access if the consent signal indicates that the user rejected the at

least one option.

15.   Cheung teaches of receiving a request for greater level of access by a client, wherein

the administrator updates the access level according to the client's request (Paragraph 0038).

16.   Cheung does not explicitly teach of denying access upon the request, but it would have

been obvious to one of ordinary skill in the art to deny access upon request to ensure the

security of the files and prevent unlimited access to all clients. Therefore, it would have been

obvious to one of ordinary skill in the art at the time the invention was made to combine the

teachings of Desai and Cheung and to deny access upon invoking an access control engine

because doing so would improve the system of Desai by providing the user with more

administrative control of data.

17.   Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Desai and

Cheung, in view of Allgeier, US Patent #5,995,972 (Allgeier hereinafter).

18.   As per claim 6, Desai does not teach the method of claim 1 further comprising:

        determining if the client has a local copy of the requested user-specific information in the

data store before transmitting the access request message; and

        retrieving said local copy of the requested user-specific information if the local is

available; determining if said local copy of the requested user-specific information is current;

and

        transmitting the access request message only if said local copy of the requested user-

specific information is not available and not current.

19.   Allgeier teaches of determining if a selected data is stored in a first database; if the

selected data is available, it is retrieved; determining if the selected data in the first database is

current; and if the selected data is not current or not available, a second database is queried

and accessed for the selected data (Col 12, lines 1-10).

20.   It would have been obvious to one of ordinary skill in the art at the time the invention was

made to combine the teachings of Desai and Cheung because the teachings of Allgeier from

Paragraph 19 would improve the system of Desai and Cheung by allowing retrieval of data from

secondary locations and by providing network efficiency by only transferring information on an

needed basis, thus preventing large amounts of data from being transferred on fixed bases.

21.   Claims 8, 10, 16-18, 36, 37, 45, and 46 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Desai and Cheung, in view of Orita, US Patent #5,163,147 (Orita

hereinafter).

22.   As per claims 8 and 36, Desai does not teach the invention, wherein determining the

intended use by the client of the requested user-specific information further comprises obtaining

a copy of an intentions document associated with the client, said intentions document including

a field being indicative of the intended use by the client of the requested user-specific

information.

23.   Orita teaches of providing information in regards to a user's intention of file access (Col

4, lines 16-18, 57-68).

24.   It would have been obvious to one of ordinary skill in the art at the time the invention was

made to combine the teachings of Desai, Cheung, and Orita because all three teachings deal

with providing granted access to data. Furthermore, the teachings of Orita to provide

information regarding a user's intention of file access would improve the system of Desai and

Cheung by using the user's intention to determine the access level of the client.

25.   As per claim 10, Desai teaches the method wherein permitting the client to have access

to the requested user-specific information in the data store if the user has granted the form of

access request by the client further comprises: permitting the client to read the requested user-

specific information in the data store (Col 9, lines 10-26. View user profile data.). However,

Desai does not teach of permitting the client to write the requested user-specific information in

the data store.

26.   Orita teaches of permitting the client to write data in the data store (Col 4, lines 16-18, 60-63).

27.   It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai, Cheung, and Orita because the teachings of Orita to permit the client to write data in the data store would enhance the system of Desai and Cheung by allowing secure modification of data stored on the network.

28.   As per claims 16, 45, and 46, Desai teaches the method of claim 15 wherein determining the intended use by the client of the certain user-specific information in the data store comprises: determining a type of information within the certain user-specific information in the data store that is being requested by the client (Col 9, lines 19-26. Elements contain certain user profile data. Col 13, lines 39-44. Element-by-element access.). However, Desai does not teach of determining a form of access to the certain user-specific information in the data store that is being requested by the client.

29.   Orita teaches of determining a form of access to data in a data store that is being requested by the client and granting identified form of access based on access control (Col 3, lines 56-69; Col 4, lines 16-19).

30.   It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai, Cheung, and Orita because the teachings of Orita to determine the a form of access to data in the data store and granting the identified form of access based on access control would enhance the system of Desai and Cheung by allowing different types of secure access to the data stored on the network such as read, write, and delete as taught by Desai.

31.   As per claim 17, Desai teaches the method of claim 16 wherein comparing the

determined intended use with the determined allowed level of access comprises: determining if

the user permits access to the type of information within the certain user-specific information in

the data store that is being requested by the client (Col 9, lines 10-18; Col 13, lines 39-44.

Grants selective access to clients.). However, Desai does not teach determining if the user

permits the form of access to the certain user-specific information in the data store that is being

requested by the client.

32.   Orita teaches of determining if the user permits the form of access to the data that is

being represented (Col 3, line2 – Col 4, lines 8; Col 4, lines 55-64).

33.   Motivation for combination is similar to claim 16. See rejection to claim 16.

34.   As per claim 18, Desai teaches the method of claim 17 further comprising: creating an

access filter, said access filter defining an extent to which the user permits access to the type of

information within the certain user-specific information in the data store and an extent to which

the user permits the form of access to the certain user-specific information in the data store (Col

10, lines 10-18; Col 13, lines 25-44. Denied or granted access by elements. Key.); and

        wherein completing the request from the client to access the certain user-specific

information in the data store when the determined intended use is within the determined allowed

level of access further comprises (Col 10, lines 10-18; Col 13, lines 25-44. Denied or granted

access by elements. Merchant access to credit information.):

applying the access filter to the user-specific information in the data store to create a

filtered information set; and permitting the client to access filtered information set (Col 10, lines

10-18; Col 13, lines 39-44. Denied or granted access by elements.).

35.   As per claim 37, Desai and Cheung teach the system of claim 36 further comprising:

a network communication device having a display interface and a selection menu and

wherein the user communicates with the web-services provider via the network communication

device (Desai: Col 8, lines 27-41. Web application. Information exchange system (IES) stores

profile data of users.); and a consent engine and generating an option list having at least one

entry therein based on the determined intended use, said consent engine displaying on the

display interface of the network communication device an option menu reflecting the generated

option list, said option menu prompting the user to accept or reject at least one option displayed

on the option menu using the selection interface of the network communication device (See

rejection to claim 1). However, Desai and Cheung do not teach of a client intentions document

and allowing or denying access based on the intention document.

36.   Orita teaches of providing information in regards to a user's intention of file access (Col

4, lines 16-18, 57-68).

37.   It would have been obvious to one of ordinary skill in the art at the time the invention was

made to combine the teachings of Desai, Cheung, and Orita because the teachings of Orita to

provide information regarding a user's intention of file access would improve the system of

Desai and Cheung by providing a method for the administrator, e.g. user, to determine the

access level of the client.

38.   Kramer teaches of protecting data in a computer system where an access list is created

based on intended use by the data manager. The data manager has the option to modify the

access list, adding or deleting users, and changing the access permissions for the users. The

access list is used to define the extent of access to the requester of the information (Col 3, lines

64-Col 4, lines 1-6, 53-55).

39.   It would have been obvious to one of ordinary skill in the art at the time the invention was

made to combine the teachings of Orita, Desai, Bradee, and Kramer because all the teachings

deal with providing selective access to information. Furthermore, the teachings of Kramer to

generating an access list to provide conditions and allowing for the change of access

permissions would improve the system of Orita, Desai, and Bradee by providing the user with

greater administrative control of its stored profile and allowing the user to determine which

clients can access the user's information.

40.   Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Desai, Cheung, and Orita, in view of Erickson et al, US Publication #2003/0081791 (Erickson

hereinafter).

41.   As per claim 11, Desai teaches the method wherein permitting the client to read the

requested user-specific information in the data store comprises accessing said requested user-

specific information and transmitting a copy of the access requested user-specific information to

the client (Col 9, lines 19-57; Col 10, lines 42-55. Access and receive user specific information.

However, Desai does not teach that the information is send in a SOAP message.

42.   Erickson teaches of transmitting messages according to the SOAP protocol (Page 2,

Paragraph 21).

43.   It would have been obvious to one of ordinary skill in the art at the time the invention was

made to combine the teachings of Desai, Cheung, and Orita because the teachings of Erikson

to use the SOAP protocol in sending messages would improve the efficiency of the system of

Desai, Cheung, and Orita by providing a simplified process of packaging data and because of

its compatibility, allowing the exchange of data over the Internet.

44.   As per claim 12, Orita teaches the method wherein permitting the client to write the

requested user-specific information in the data store comprises receiving at the host computer a

message from the client identifying the requested user-specific information and writing the

identified requested user-specific information in the data store (Col 3, lines 57-60; Col 4, lines

61-68; Col 5, lines 8-13. Receive request for the information and writing the identified

information. Permit client to write the information in the host computer.). However, Orita does

not teach of receiving at the web-services provider a SOAP message from the client.

45.   Erickson teaches of transmitting messages according to the SOAP protocol (Page 2,

Paragraph 21).

46.   It would have been obvious to one of ordinary skill in the art at the time the invention was

made to combine the teachings of Desai, Cheung, and Orita because the teachings of Erikson

to use the SOAP protocol in sending messages would improve the efficiency of the system of

Desai, Cheung, and Orita by providing a simplified process of packaging data and because of

its compatibility, allowing the exchange of data over the Internet.

47.   Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Desai and

Cheung, in view of Kramer, US Patent #5,414,852 (Kramer hereinafter).

48.   As per claim 13, Desai and Cheung teaches the method wherein updating the access control list to permit the client to have access to the requested user-specific information in the data store if the default access control instruction permits the determined intended use further comprises: updating the access control list to permit the client o read the requested user-specific information in the data store (Cheung, Paragraph 0038). However, Desai and Cheung do not teach updating the access control list to permit the client to write the requested user-specific information in the data store.

49.   Kramer teaches wherein the access list is updated to permit the client to read and write the requested data file (Col 4, lines 49-55).

50.   It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai, Cheung, and Kramer because all three teachings deal with providing selective access information. Since Cheung teaches of updating the access level to allow access to data in response to a client request, it would also be desirable to update the access level to permit writing the data as taught by Kramer. Doing so would enhance the system of Desai and Cheung by providing the user with greater administrative control of clients the type of access clients are permitted, and allowing clients to modify data over the network.

51.   Claims 22, and 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Desai, in view of Kramer.

52.   As per claims 22 and 28, Desai teaches substantial features of the claimed invention including a user-centric method and computer media with instructions (Col 11, lines 27-46.) for controlling access to user specific information in a network computing environment, said

network computing environment including a web-services provider and a user of a service

provided by the web-services provider, the web-services provider maintaining a data store of

user specific information associated with the user (Col 8, lines 27-41. Web application.

Information exchange system (IES) stores profile data of users.), said user-specific information

accessible by the user and having access by the clients controlled by the user (Col 9, lines 10-

17. User selectively grants data by element-by-element basis to third parties.), the user

communicating with the web-services provider via a network communication device having a

display interface and a selection interface, said user-centric method of controlling access to a

user-specific information comprising:

identifying the user (Col 8, lines 27-41. User.);

identifying a plurality of clients of the web-services provider wherein the user desires to

grant access to the user-specific information in the data store to certain of the plurality of clients

(Col 9, lines 10-31; Col 14, line 20-27, 63-67. Third parties request access to user profile.);

identifying a level of access to the user-specific information in the data store the user

desires to impose on the certain clients (Col 9, lines 1-18; Col 13, lines 39-52; Col 15, lines 1-

12. Access is granted by element-by-element basis.);

exposing a menu to the user on the display interface of the network communication

device, said menu allowing the user to identify the certain clients, and the level of access (Col 8,

lines 63-67; Col 13, lines 19-37. User communicates with IES to identify third parties and level

of access. Menu, display interface is inherent.); and

transmitting information indicating the identified certain clients, and the level of access to

the web-services provider in a digital message format (Col 8, lines 63-67; Col 13, lines 19-37.

User communicates with IES to selectively grant access.); and

writing an access control rule to an access control list associated with said data store, said access control rule limiting access to the user-specific information in the data store by the certain clients to the identified method of access and the identified level of access (Col 13, lines 25-45; Col 14, lines 1-4. Limit to third parities to certain elements.).

53.   Desai does not teach:

identifying a method of access by which the user is willing to allow the certain clients to access the user-specific information in the data store;

exposing a menu to the user on the display interface of the network communication device, said menu allowing the user to identify method of access;

transmitting information indicating the identified method of access.

54.   Kramer teaches of identifying a method access by which user is willing to allow the certain clients to access information; allow the user to identify the method of access; and modify the access list (Col 4, lines 1-5, 53-55)

55.   It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai and Kramer because the teachings of Desai to identify a method of access allowed by the user and modifying the access list according to the identified method of access would improve the system of Desai by providing users with more administrative responsibility of data stored on the network..

56.   As per claim 25, Desai does not teach the method of claim 22 wherein identifying the method of access further comprises identifying whether the certain clients is permitted to modify the user-specific information in the data store.

57.   Kramer teaches of identifying whether the user permits clients to modify files in a data store (Col 4, lines 1-5, 52-55).

58.   Motivation for combining references is similar to claim 22. See rejection to claim 22.

59.   As per claim 26, Desai teaches the method of claim 22 wherein identifying the level of access further comprises grouping the user-specific information in the data store into a plurality of information types and identifying which of said plurality of information types the certain clients may access (Col 9, lines 10-30. The user-specific information in the data store is grouped and identified as to which information the client may access. Vendor may access telephone number and credit card number, while business contact may just view the user's telephone number.).

60.   As per claim 27, Desai does not teach the method of claim 22 further comprising: authenticating a digital identity of the user prior to writing the access control rule to the access control list associated with the data store of user-specific information; and writing the access control rule to said access control list if the digital identity of the user is authenticated.

61.   Kramer teaches of providing an identifier to access information on a computer system, wherein the data manager controls an access list, which contains the identifiers of the users. The data manager may provide write access based on the user's authorized access. The data manager application is invoked when user desires to access to files (Col 3, lines 15-34; Col 4, lines 49-55).

62.   It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai and Kramer because the teachings of Kramer to perform the above method of paragraph 61 would improve the system of Desai by providing

security of data stored on the network by preventing unauthorized users to different forms of

access.

63.   Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Desai and

Kramer, in view of Robertson, US Patent #6,269,369 (Robertson hereinafter).

64.   As per claim 23, Desai teaches of selectively granting access to one or more third

parties to user's stored profile and sending to the third parties (Col 9, lines 42-51). However,

Desai does not teach the method of a subscription status indicating whether the user intends

the certain clients to be notified if the user-specific information in the data store changes.

65.   Robertson teaches of a contact management system, wherein clients may be permitted

access to user's stored profile information. The contact manager determines whether any of the

user's contacts need to be notified of changes to the user's information (Col 6, lines 48-54; Col

8, lines 17-23, 57-61).

66.   It would have been obvious to one of ordinary skill in the art at the time the invention was

made to combine the teachings of Desai, Kramer, and Robertson because all three teachings

deal with providing controlled access to stored information, while both Desai and Robertson

specifically deal with selective access to user's profile information. Furthermore, the teachings

of Robertson to perform the above method of claim 14 would improve the system of Desai and

Kramer by allowing the user's clients to have the most up-to-date information regarding the user

and allowing the user to select clients that would receive notifications.

67.   Claims 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, in

view of Desai, Bradee, US Publication #2002/0095571 (Bradee hereinafter), and Cheung.

68.   As per claims 42 and 43, Orita teaches substantially the invention as claimed including a

method and computer-readable media (Col 3, lines 10-32. Computer.) for selectively allowing

access to files over a computer network. Orita's teachings comprise of:

retrieving an intentions document associated with the third party desiring access to the

certain information in the data store, said intentions document identifying (Col 3, lines 10-14; Col

3, lines 15-20, 56-61. Clients sends request to access specific files.):

a purpose for which the third party desires access to the certain information in the data

store (Col 3, lines 56-65; Col 4, lines 16-19. Client indicates the type of access such as

deleting, modifying, write-in, and readout.);

a method by which the third party proposes to access the certain information in the data

store (Col 3, lines 56-65; Col 4, lines 16-19. Client indicates the type of access such as

deleting, modifying, write-in, and readout.);

.   an identity of the third party (Col 3, lines 10-13, lines 56-61. User provides ID and

password.);

the certain information in the data store to which the third party desires access (Col 3,

lines 10-14; Col 3, lines 15-20, 56-61. Clients sends request to access specific files.);

the purpose for which the third party desires access to the certain information in the data

store (Col 3, lines 56-65; Col 4, lines 16-19. Client indicates the type of access.);

the method by which the third party proposes to access the certain information in the

data store (Col 3, lines 56-65; Col 4, lines 16-19. Client indicates the type of access.);

69.   Orita does not teach that the information is user-specific information, a web-services

provider maintaining a data store of the user-specific information;

a value proposition associated with the purpose for which the third party desires access the data in the data store,

the value proposition associated with the purpose for which the third party desires access to the data in the data store; and

generating a set of menu entries in response to the third party's proposal; displaying the menu entities on the menu on the display interface of the network communication device;

prompting the user to authorize or deny the third party to access the certain information in the data store; and

operatively receiving a selection signal being indicative of whether the user authorized or denied the third party to access the certain information in the data store, and creating an access control rule indicative of whether the user authorized the third party to access the user-specific information in the data store.

70.   Desai teaches of providing user-specific information to clients, where the user selectively grants access to the user's user-specific information to one or more clients on an element-by-element basis (Col 9, lines 10-18), and wherein the user's user-specific information is stored on an information exchange server, accessible through the Internet (Col 8, lines 27-41).

71.   It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Desai because both teachings deal with providing selectively access to certain information stored on a database to one of more clients. Furthermore, the teachings of Desai for the information to be user-specific; allowing access to certain information; and storing user-specific information on a web server would enhance the teachings of Orita by providing different type of data stored on the network to accessible by clients, and allowing the data to be more accessible by web browsers.

72.   Bradee teaches of selectively allowing access to information stored on a web server

where the client pays to view the information. Bradee also teaches of dynamically updating the

access list to allow the client access to the stored information (Page 8, Paragraph 0062)

73.   It would have been obvious to one of ordinary skill in the art at the time the invention was

made to combine the teachings of Orita, Desai, and Bradee because all three teachings deal

with providing selective access to information over computer network. Furthermore, the

teachings of Bradee for the user to offer a value proposition and to dynamically update the user

access list would improve the system of Orita and Desai by allowing clients to access certain

information on the web server when the client meets conditions set forth by the user.

74.   Cheung teaches of invoking an access control engine in response to the client's request

if the client has not been granted the form of access; updating the access control list to permit

the client to have access to the requested information; requesting the administrator that the

access level be changed to allow for greater access; and updating the access level according to

the client's request (Paragraph 0038).

75.   It would have been obvious to one of ordinary skill in the art at the time the invention was

made to combine the teachings of Orita, Desai, Bradee, and Cheung because the teachings of

Cheung from the above Paragraph 74 would improve the system of Orita, Desai, and Bradee by

providing dynamic changing of clients' access levels and providing more control of information

by the user.

Conclusion

76.   A shortened statutory period for reply to this Office action is set to expire THREE

MONTHS from the mailing date of this action.

77.   Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Joshua Joo whose telephone number is 571 272-3966. The examiner can

normally be reached on Monday to Thursday 8AM to 5PM and every other Friday.

78.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, John A. Follansbee can be reached on 571 272-3964. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

79.   Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

February 17, 2006
JJ

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100